REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	12/29/05	Final Progress--July 1, 2001--December 31, 2004

4. TITLE AND SUBTITLE
Algorithmic Speedup from Quantum Mechanics

5. FUNDING NUMBERS
DAAD19-01-1-0656

6. AUTHOR(S)
Edward Farhi and Jeffrey Goldstone

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Laboratory for Nuclear Science, Massachusetts Institute of Technology
77 Massachusetts Avenue, Cambridge MA 02139

8. PERFORMING ORGANIZATION REPORT NUMBER
MIT Account Number: 6892311

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
42687.9-PH-QC

11. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12 b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

This project was concerned primarily with one central theme which is the attempt to use quantum mechanics to design algorithms that perform better than conventional (non-quantum) algorithms for solving certain problems. We looked at a variety of approaches. The first is quantum adiabatic evolution which was invented by the authors along with M. Sipser and S. Gutmann. During the period of this report we studied the robustness of this algorithm, generalized the algorithm beyond its original specification and also showed that it can outperform classical algorithms in certain settings. We also investigated continuous time quantum walks which were introduced as a quantum algorithmic tool by Farhi and Gutmann. Here the high point was the discovery of a quantum walk algorithm that gives provable exponential speedup over the best possible classical algorithm for a certain oracle problem. Goldstone and Childs (a graduate student at MIT at the time) explored the use of quantum walk algorithms for searching a spatial grid. Also Farhi, Goldstone and coworkers showed how to use repeated measurements as an algorithmic tool. In particular we showed how to achieve the Grover square root speedup using measurement algorithms.

14. SUBJECT TERMS
Quantum Computing, Quantum Algorithms, Quantum Walk, Quantum Adiabatic Algorithms

15. NUMBER OF PAGES
6

16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	**UNCLASSIFIED**	**UNCLASSIFIED**	**UL**

NSN 7540-01-280-5500

Standard Form 298 (Rev.2-89)
Prescribed by ANSI Std. 239-18
298-102

Enclosure 1

Final Progress Report:

Algorithmic Speedup from Quantum Mechanics

July 1, 2001 to December 31, 2004

Edward Farhi and Jeffrey Goldstone
Center for Theoretical Physics
Department of Physics and Laboratory for Nuclear Science
Massachusetts Institute of Technology

This project was concerned primarily with one central theme which is the attempt to use quantum mechanics to design algorithms that perform better than conventional (non-quantum) algorithms for solving certain problems. We looked at a variety of approaches. The first is quantum adiabatic evolution which was invented by the authors along with M. Sipser and S. Gutmann. During the period of this report we studied the robustness of this algorithm, generalized the algorithm beyond its original specification and also showed that it can outperform classical algorithms in certain settings. We also investigated continuous time quantum walks which were introduced as a quantum algorithmic tool by Farhi and Gutmann. Here the high point was the discovery of a quantum walk algorithm that gives provable exponential speedup over the best possible classical algorithm for a certain oracle problem. Goldstone and Childs (a graduate student at MIT at the time) explored the use of quantum walk algorithms for searching a spatial grid. Also Farhi, Goldstone and coworkers showed how to use repeated measurements as an algorithmic tool. In particular we showed how to achieve the Grover square root speedup using measurement algorithms. In the remainder of the report we will elaborate on these findings and make reference to the associated papers.

Adiabatic Algorithms

The original idea of quantum adiabatic algorithms is to use a quantum computer to find the solution to a combinatorial search problem. An instance of the problem is specified by a list of clauses (or constraints) on the 2^n values taken by n bits. Typically we are interested in problems such at 3SAT where the clauses each involve only 3 bits. We want to find the assignment of the bits that satisfies the most clauses. To do so we construct a cost function which is a sum of terms, one for each clause. Each clause cost functions takes the value 1 if the clause is not satisfied and 0 if it is. The assignment which minimizes the

number of violations corresponds to the lowest value of the cost function. Hence we want to find the minimum of the cost function. We specify a Hamiltonian, H_P, which is diagonal in the computational basis and is equal to the cost function acting on the computational basis states. We now want to find the ground state of this Hamiltonian. To do so we introduce another Hamiltonian, H_B, which is easy to construct and whose ground state we know. We imagine we have the ability to interpolate between these Hamiltonians, say by constructing $H(s) = (1-s) * H_B + s * H_P$ for all s between 0 and 1. We start our computation in the known ground state of H_B and then allow the Hamiltonian to change as the quantum state evolves in time. If we pick $s(t)$ to be sufficiently slowly varying then the evolving quantum state will remain in the ground state of $H(s)$. When s reaches 1 we are in the ground state of H_P and have the answer to our problem. The computational issue is how slow we must go. This in turn depends on the gap which is the minimum (over s) of the difference between the ground state energy and the first excited state energy of $H(s)$. If the gap is big the run time can be short and if the gap is small the run time must be long.

This adiabatic approach to computation appears to be intrinsically robust against error if the quantum computer actually is governed by the Hamiltonian $H(s)$ and the system is kept cold. This was studied in detail in reference [7]. Here two types of error were investigated. The first is due to control errors. Remarkably if the route from the initial Hamiltonian to the problem Hamiltonian is not followed but the problem Hamiltonian is reached, there is no reason to think that the algorithm will not perform as well as intended as long as the conditions for adiabaticity are maintained. This was demonstrated numerically (on systems with very few qubits) where it was seen that sometimes varying from the intended path can increase the success probability of the algorithm! In this paper decoherence was also studied using a Lindblad equation to incorporate the effects of coupling to the environment. The small size systems numerically also showed what we expected. If the temperature was kept low compared to the minimum gap, the effects of the environment were negligible.

A criticism leveled against the quantum adiabatic algorithm was that it is nothing other than simulated annealing (a classical algorithm) in disguise. To demonstrate the quantum nature of the algorithm, which indeed gives it additional power, we constructed examples of search problems where simulated annealing with local update rules would necessarily fail but the quantum adiabatic algorithm succeeds in polynomial time in finding the minimum of a cost function. (See reference [6].) This paper quieted down the objection that the quantum adiabatic algorithm was performing as a classical algorithm.

There were attempts to show that the quantum adiabatic algorithm would necessarily fail on certain simple instances of satisfiability where the constraints are all local, that is, each clause contains only three bits. In fact Umesh Vazirani and collaborators did construct such an example which we confirmed looked problematic for the quantum algorithm. However in reference [4] we introduced the idea that the adiabatic algorithm should be run repeatedly on each instance of a problem where each repetition uses a different

path in Hamiltonian space between H_B and H_P. We gave some simple rules for randomly generating interpolating paths. With these rules we showed that the quantum adiabatic algorithm would in fact solve in polynomial time the instances introduced by Vazirani and collaborators. If the algorithm is always run by choosing a random interpolating path between H_B and H_P and it seems to us very challenging to find a convincing counterexample. Of course this still does not shed light on the more interesting question of whether there exists an interesting set of instances for which we can demonstrate algorithmic success. The counterexamples were contrived and we feel did not ultimately shed light on the question of whether the algorithm could be successful in interesting cases, especially since the counterexamples were defeated.

In a slightly different vein we looked at the possibility of doing quantum search by measurement. (See reference [5].) Again the idea is to do ground state quantum computing. But now the system is kept in its ground state by measuring the energy repeatedly. The idea is that if you are in the ground state of $H(s)$ and you then measure the operator $H(s+\delta)$, if δ is small, you will most likely obtain the ground state of $H(s+\delta)$. By repeating this you can move from the ground state of $H(0)$ to the ground state of $H(1)$ as in the adiabatic algorithm. We analyzed the requirements for this type of computation in terms of the minimum gap. We also showed how to solve the Grover problem by making only two measurements on a particular Hamiltonian. We showed that the minimum time required to perform the measurements grows as $\sqrt{N}$ so, as expected, speedup beyond Grover speedup is not achieved.

We now turn to quantum walk. The idea of using quantum walk as an algorithmic tool was first introduced by Farhi and Gutmann in 1997. In this work it was also shown that a quantum walk could move across a graph exponentially faster than the associated classical random walk on the same graph. In reference [3] these ideas were put to use to obtain a provable algorithmic speedup for a quantum algorithm over the best possible classical algorithm for a particular oracle problem. The ideas was to take a graph with an exponential number of nodes with two marked as Entrance and Exit. The graph is given in the form of an oracle which means that each node of the graph has a name which offers no information about the node's location in the graph and when the oracle is offered the name of node it returns the names of the nodes connected to the input node. The goal is to devise a strategy which will allow you to go from the Entrance node and arrive at the Exit node. Given the devious form of the graph we could show that no classical algorithm could achieve this with a subexponential number of queries to the oracle. However a quantum walk algorithm on the same structure, using the same rules, arrives at Exit in polynomial time. Among other things, we had to show how to turn oracle calls into Hamiltonian evolution. This is one of very few examples of provable speedup by a quantum algorithm over the best possible classical algorithm. Furthermore the speedup is exponential.

Goldstone and Childs (who was Farhi's graduate student at the time) looked at continuous time quantum walks as a method for searching a database which is laid out in d spatial dimensions. (See reference [2].) They showed that they could obtain the square

root of N speedup only for d larger than 4. In this case there was one quantum basis state for each node in the grid. However by extending the Hilbert space to include a spin degree of freedom they were able to show that they could obtain Grover speedup for d larger than 2 and they got $\sqrt{N} \times \log(N)$ speedup in two spatial dimensions. The latter work made use of a spatially discrete version of the Dirac Hamiltonian which describes a relativistic particle with spin.

In summary during the three years of this project we made many advances in our understanding of quantum adiabatic algorithms and also of quantum walk algorithms. We engaged many collaborators and in particular wrote five papers with a terrific graduate student, Andrew Childs.

The following references are a complete list of the publications and articles on http://arxiv.org, which came out during the period of this report.

References

[1] A. M. Childs and J. Goldstone, "Spatial search and the Dirac equation", *Phys. Rev. A* **70**, 042312 (2004), [arxiv: quant-ph/0405120].

[2] A. M. Childs and J. Goldstone, "Spatial search by quantum walk", *Phys. Rev. A* **70**, 022314 (2004), [arxiv: quant-ph/0306054].

[3] A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann and D. A. Spielman, "Exponential algorithmic speedup by quantum walk", Proc. 35th ACM Symposium on Theory of Computing (STOC 2003), pp. 59-68 [arxiv: quant-ph/0209131].

[4] E. Farhi, J. Goldstone and S. Gutmann, "Quantum Adiabatic Evolution Algorithms with Different Paths", [arxiv: quant-ph/0208135].

[5] A. M. Childs, E. Deotto, E. Farhi, J. Goldstone, S. Gutmann and A. Landahl, "Quantum search by measurement" *Phys. Rev. A* **66**, 032314 (2002) [arxiv: quant-ph/0204013].

[6] E. Farhi, J. Goldstone and S. Gutmann, "Quantum Adiabatic Evolution Algorithms versus Simulated Annealing", [arxiv: quant-ph/0201031].

[7] A. M. Childs, E. Farhi and J. Preskill, "Robustness of adiabatic quantum computation", *Phys.Rev. A* **65**, 012322 (2002), [arxiv: quant-ph/0108048].